



HW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Matthew Conover et al.
Assignee: Symantec Corporation
Title: METHOD AND APPARATUS TO DETECT AND RECOVER FROM A
STACK FRAME CORRUPTION
Serial No.: 10/803,848 Filed: March 17, 2004
Examiner: Unassigned Group Art 2183
Unit:
Docket No.: SYMC1049

Monterey, CA
June 10, 2004

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT UNDER §1.97(b)

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, Applicants wish to call the following documents (a copy of each is enclosed) to the attention of the Examiner:

OTHER DOCUMENTS:

1)	Chien, E. and Szor, P., "Blended Attacks Exploits, Vulnerabilities and Buffer-overflow Techniques in Computer Viruses", Virus Bulletin Conference, September 2002, pp. 1-36.
2)	Huang, Yinrong, "Protection Against Exploitation of Stack and Heap Overflows", Exurity, Inc., Canada, April 11, 2003, pp. 1-10 [online]. Retrieved on June 9, 2004. Retrieved from the Internet: <URL:http://www.cgisecurity.com/lib/AntiOverflows.pdf>.
3)	No author, "Immunix Canary Patch to GCC 2.7.2.2 -- A Buffer Overflow Exploit Detector", pp. 1-4 [online]. Retrieved on February 10, 2004. Retrieved from the Internet: <URL:http://www.ussrback.com/UNIX/utilities/stackguard/stackguard-gcc.README>.

A PTO form 1449 listing these documents is enclosed.

Citation of the above documents shall not be construed as:

1. an admission that the document is necessarily prior art with respect to the instant invention;
2. a representation that a search has been made, other than as described above; or
3. an admission that the information cited herein is, or is considered to be, material to patentability as defined in § 1.56(b).

If the USPTO issued a first office action prior to the mailing date of this paper, the Commissioner is hereby authorized to charge any fees required for consideration of this Information Disclosure Statement, and to credit any overpayment of fees to Deposit Account No. 50-0553.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on June 10, 2004.



Attorney for Applicant(s)

June 10, 2004

Date of Signature

Respectfully submitted,



Lisa A. Norris
Attorney for Applicants
Reg. No. 44,976
(831) 655-0880

Form PTO-1449

Atty Docket No.

Serial No.

SYMC1049

10/803,848

**INFORMATION DISCLOSURE CITATION
IN AN APPLICATION**

Applicant(s)

Matthew Conover et al.

Filing Date

March 17, 2004

Group

2183

(Use several sheets if necessary)

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

AR	Chien, E. and Szor, P., "Blended Attacks Exploits, Vulnerabilities and Buffer-overflow Techniques in Computer Viruses", Virus Bulletin Conference, September 2002, pp. 1-36.
AS	Huang, Yinrong, "Protection Against Exploitation of Stack and Heap Overflows", Exurity, Inc., Canada, April 11, 2003, pp. 1-10 [online]. Retrieved on June 9, 2004. Retrieved from the Internet: <URL:http://www.cgisecurity.com/lib/AntiOverflows.pdf>.
AT	No author, "Immunix Canary Patch to GCC 2.7.2.2 -- A Buffer Overflow Exploit Detector", pp. 1-4 [online]. Retrieved on February 10, 2004. Retrieved from the Internet: <URL:http://www.ussrback.com/UNIX/utilities/stackguard/stackguard-gcc.README>.

Examiner

Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).